

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de IBM WebSphere

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-126>

Gestion du document

Référence	CERTA-2009-AVI-126
Titre	Vulnérabilités de IBM WebSphere
Date de la première version	01 avril 2009
Date de la dernière version	-
Source(s)	Bulletin de sécurité IBM swg24022549 du 26 mars 2009
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

IBM WebSphere 7.x.

3 Résumé

Plusieurs vulnérabilités présentes dans IBM WebSphere permettent à un utilisateur malveillant de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités sont présentes dans IBM WebSphere :

- la première, dans la console d'administration, permet de réaliser de l'injection de code indirecte (XSS) ;

- un correctif intermédiaire positionne des droits d'accès à des fichiers de manière incorrecte, donnant accès en exécution à tout utilisateur ;
- une erreur non précisée permet de voler la session d'un utilisateur ;
- une erreur non précisée est présente dans la définition des signature numériques XML.

5 Solution

Le correctif 7.0.0.3 remédie à ces vulnérabilités.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité IBM swg24022549 du 26 mars 2009 :
<http://www-01.ibm.com/support/docview.wss?uid=swg24022549>
- Référence CVE CVE-2009-0892 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0892>
- Référence CVE CVE-2009-1173 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1173>
- Référence CVE CVE-2009-1174 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1174>

Gestion détaillée du document

01 avril 2009 version initiale.